REMARKS

Prior to this communication, claims 1 – 29 were pending. In the pending Action, the Examiner rejected claims 1 – 29. Examination and reconsideration in view of the remarks contained here in are respectfully requested.

Claim Rejections

35 U.S.C. § 101 Rejections

Claims 7, 8, and 12 – 19 stand rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter. Particularly, the Office contends that "the language in the specification ([0018]) raises an issue because the claims are directed merely to an abstract idea that is not tied to an article of manufacture which would result in practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter." (Page 3 of Action mailed April 19, 2007.)

Claims 7, and 8 depend from claim 1, while claims 13 – 19 depend from claim 12.

Before addressing the Office's position in detail, it is helpful to identify the problem addressed by the present invention. With reference to Internet use, which is one area in which the present invention may prove helpful, there are a huge number of users accessing password-protected sites every day on a worldwide basis. These users often have accounts at multiple sites, and it is recognized by many as good practice to have a unique, random password at each site. The problem presented under such circumstances is how to manage the many unique passwords. The present invention provides a system and method for managing a list of passwords, and thus the invention produces a useful, tangible, and concrete result. It addresses a practical need shared by many people in today's information age, particularly with respect to password-protected Internet sites. The use of an encryption module as part of such system and method does not render the underlying system and method unuseful, intangible, or non-concrete. For example, if the Examiner accepts that claim 1 meets the requirements of 35 USC 101 (and this we infer from the Examiner not rejecting claim 1 on such grounds), the fact that claim 7 further specifies that "the host computing processor comprises an encryption module configured to encrypt the list of passwords" does not suddenly make the useful, tangible, concrete system of claim 1 evaporate. In other words, the

usefulness of storing and communicating a list of encrypted passwords in claim 1 is not eviscerated by the implementation of an encryption module to encrypt the list of passwords.

With respect to the specific basis of the Office's Section 101 rejection, the Office notes that the claims are directed to "an encryption module," and that language in the specification ([0018]) "raises an issue because the claims are directed merely to an abstract idea that is not tied to an article of manufacture which would result in practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter." (Page 3 of Action mailed April 19, 2007.) Paragraph [0018] indicates that "the encryption module 128 includes an encryption algorithm that can be implemented with either software or hardware." It is unclear to Applicant why any of the language raises any issues. It is very common for a computer to include software or firmware that implements an algorithm. For example, a Microsoft® Windows-based personal computer typically includes a media player that decodes and plays an mp3-based program, such as, for example, songs. All of the above-identified elements – Microsoft® Windows-based personal computer, media player, and mp3-based programs – are not abstract ideas. Rather, these elements are all articles of manufacture. The elements produce a concrete, useful, and tangible result – decoding and playing an encoded song, for example.

The determination to be made is whether **the claims** produce a useful, concrete, and tangible result. This principal was annunciated in *State Street Bank & Trust Co. v. Signature Financial Group Inc.*, 149 F.3d 1368 (Fed. Cir. 1998), in which the Court noted the following:

> After *Diehr* and *Chakrabarty*, the Freeman-Walter-Abele test has little, if any, applicability to determining the presence of statutory subject matter. As we pointed out in *Alappat*, 33 F.3d at 1543, 31 USPQ2d at 1557, application of the test could be misleading, **because a process, machine, manufacture, or composition of matter employing a law of nature, natural phenomenon, or abstract idea is patentable subject matter even though a law of nature, natural phenomenon, or abstract idea would not, by itself, be entitled to such protection**. The [Freeman-Walter-Abele] test determines the presence of, for example, an algorithm. Under *Benson*, this may have been a sufficient indicium of nonstatutory subject matter. However, after *Diehr* and *Alappat*, the mere fact that a claimed invention involves inputting numbers, calculating numbers, outputting numbers, and storing numbers, in and of itself, would not render it nonstatutory subject matter, unless, of course, its operation does not produce a "useful, concrete and tangible result." *Alappat*, 33 F.3d at 1544, 31 USPQ2d at 1557. After all, as we have repeatedly stated, **every step-by-step**

> **process, be it electronic or chemical or mechanical, involves an algorithm in the broad sense of the term. Since § 101 expressly includes processes as a category of inventions which may be patented and § 100(b) further defines the word "process" as meaning "process, art or method, and includes a new use of a known process, machine, manufacture, composition of matter, or material," it follows that it is no ground for holding a claim is directed to nonstatutory subject matter to say it includes or is directed to an algorithm.** This is why the proscription against patenting has been limited to mathematical algorithms . . . . *In re Iwahashi*, 888 F.2d 1370, 1374, 12 USPQ2d 1908, 1911 (Fed. Cir. 1989) (parenthetical omitted).
>
> **The question of whether a claim encompasses statutory subject matter should not focus on which of the four categories of subject matter a claim is directed to —process, machine, manufacture, or composition of matter—<u>but rather on the essential characteristics of the subject matter, in particular, its practical utility.</u>** . . . For purpose of our analysis, as noted above, claim 1 is directed to a machine programmed with the Hub and Spoke software and admittedly produces a "useful, concrete, and tangible result." *Alappat*, 33 F.3d at 1544, 31 USPQ2d at 1557. This renders it statutory subject matter, even if the useful result is expressed in numbers, such as price, profit, percentage, cost, or loss.

Id. at 1373-75 (emphasis added).

With respect to "an encryption module" being an abstract idea, the foundation of encryption is linguistic. For example, a famous linguistic implementation of encryption was the basis of the film "Wind Talkers," which dramatizes the achievements of radio communicators speaking in Cherokee to confuse Japanese code breakers in World War II. More importantly, encryption is not abstract idea such as, for example, the geometric constructs that were found to exist in the claims at issue in *In re Warmerdam* 33 F.3d 1354, 1360 (Fed. Cir. 1994). In *Warmerdam*, the Court analyzed the following claim.

> 1. A method for generating a data structure which represents the shape of [sic] physical object in a position and/or motion control machine as a hierarchy of bubbles, comprising the steps of:
>
> first locating the medial axis of the object and
>
> then creating a hierarchy of bubbles on the medial axis

The *Warmerdam* Court noted that "it appears [that] the only practical, embodiment of the claimed method involves steps which are essentially mathematical in nature, i.e., utilization of the Hilditch Skeletonization method to locate the medial axis, followed by utilization of a top-down or bottom-up procedure for creating the bubble hierarchy. In this

sense, at least, the claim is mathematical in nature. (footnote omitted)" *Id.* Thus, it was clear that the claimed subject matter was related to an algorithm. With respect to certain embodiments disclosed in Applicant's specification it is clear that they involve password management through various mechanisms (see, e.g., Background of the Invention). Thus, the embodiments are more than abstract ideas or exercises.

The *Warmerdam* Court also noted that

> **regardless whether the claim can be said to recite indirectly or directly a mathematical algorithm, the dispositive issue for assessing compliance with Section 101 in this case is whether the claim is for a process that goes beyond simply manipulating "abstract ideas" or "natural phenomena."** (footnote omitted) The body of claim 1 recites the steps of "locating" a medial axis, and "creating" a bubble hierarchy. These steps describe nothing more than the **manipulation of basic mathematical constructs**, the paradigmatic "abstract idea."

Id. at 1360 (emphasis added). In contrast, and as noted, claim 7 is directed to managing passwords - not, for example, manipulating geometric constructs such as axes.[1]

As should be apparent from the above, the premise that an encryption module is an abstract idea is erroneous. However, even if such a characterization is correct, the claim calls for encryption be applied to passwords and encrypted passwords be stored. Password is tangible and storage of it is useful. Since the claim goes beyond mere manipulation of abstract idea it falls within the scope of Section 101.

Similarly, claims 12 – 19 require an encryption module that is not an abstract idea for at least the reasons set forth above with respect to claims 7 and 8. Rather, claims 12 – 19 recite subject matter that produces useful, concrete, and tangible results, such as, managing passwords.

As a consequence, Applicant submits that claims 7, 8 and 12 – 19 as originally submitted define statutory subject matter. The claims recite subject matter that produces a useful, concrete, and tangible management of passwords.

[1] It should be noted that *Warmerdam* was decided using the now discredited Freeman-Walter-Abele test and that a Court using the currently accepted analysis may have ruled that even the claim in the *Warmerdam* case meets the requirements of Section 101.

35 U.S.C. § 102 Rejections

Claims 1, 2, 4 – 7, 9, 10, 12, 14 – 17, 20, 21, 23 – 25, 27, and 28 stand rejected under 35 U.S.C. § 102 (a/e) as being anticipated by U.S. Patent Application No. 2003/0046567 ("Carman").

Claim 1 and Dependent Claims 1, 2, 4 – 7, 9, and 10

Claim 1 is directed to a password management system that includes, among other things:

- a host computing processor
    - having a peripheral port.
    - operable to encrypt a list of passwords.
- a portable access device
    - adapted to be coupled to the host computing processor.
    - storing the list of encrypted passwords.
    - communicating the list of encrypted passwords with the host computing processor through the peripheral port.

Carman does not anticipate claim 1.

Rather, Carman discloses a memory card 100 having a controller 105 therein. After the memory card 100 has been attached to a cellular telephone 200, the controller 105 on the memory card 100 decrypts passwords stored in a memory 110 on the memory card 100. Once decrypted, a username and a password associated with a URL are transmitted to the cellular telephone 200. (Paragraph [0022], and FIG. 2.) Furthermore, Carman discloses that "**the cellular telephone's processor** provides the necessary control to **store and recall** the usernames and their associated passwords." (Paragraph [0023], emphasis added.) Carman, therefore, does not anticipate at least with respect to "a host computing processor having a peripheral port, and operable to encrypt the list of passwords," as recited in claim 1.

Claim 1 is therefore not anticipated by Carman, and Applicant respectfully requests withdrawal of the rejection of claim 1. Claims 1, 2, 4 – 7, 9, and 10 depend from claim 1, and therefore, are allowable for at least the reasons set forth above.

Claim 12 and Dependent Claims 14 – 17

Claim 12 is directed to a password management system. The system is coupled to a computer having access to at least one account that has a password associated therewith. The password management system includes:

- a portable access device storing in a rewritable memory a list of encrypted passwords for the at least one account.

- an encryption module executed on the computer and operable to encrypt a new password for addition to the list of passwords.

- a driver coupled to the encryption module and operable to read a master access code, the driver decrypting the list of encrypted passwords from the portable access device using the master access code and updating the list of encrypted passwords with the new encrypted password.

As noted above with respect to claim 1, Carman does not anticipate at least with respect to "an encryption module executed on the computer and operable to encrypt a new password for addition to the list of passwords," as recited in claim 12. Applicant respectfully requests withdrawal of the rejection of claim 12. Claims 14 – 17 depend from claim 12, and therefore, are allowable for at least the reasons set forth above.

Claim 20 and Dependent Claims 21, 23 – 25, 27, and 28

Claim 20 is directed to a method of managing a list of passwords. The method includes, among other things:

- encrypting a list of passwords at a host computing processor.

- storing the list of encrypted passwords at a portable access device selectively coupled to the host computing processor.

- communicating the at least one encrypted password between the host computing processor and the portable access device.

As noted above with respect to claims 1 and 12, Carman does not anticipate at least with respect to "encrypting a list of passwords at a host computing processor," as recited in claim 20. Applicant respectfully requests withdrawal of the rejection of claim 20. Claims 21, 23 – 25, 27, and 28 depend from claim 20, and therefore, are allowable for at least the reasons set forth above.

35 U.S.C. § 103 Rejections

Claims 8, 18, and 26

Claims 8, 18, and 26 stand rejected under 35 U.S.C. § 103 (a) as being unpatentable over Carman.

To establish a *prima facie* case of obviousness, three basic criteria must be met. *M.P.E.P.* § 706.02(j), and 2143.

> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine the reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must be both found in the prior art, not in applicant's disclosure.

Id. See also In re Rougget, 149 F.3d 1350, 1355 (Fed. Cir. 1998) ("To reject claims in an application under section 103, the Examiner must show an unrebutted *prima facie* case of obviousness. In the absence of a proper *prima facie* case of obviousness, an applicant who complies with the other statutory requirements is entitled to a patent.")

The Office has not set forth a proper *prima facie* case of obviousness.

As noted above with claim 1, Carman makes no mention of, among other things, "a host computing processor having a peripheral port, and operable to encrypt the list of passwords," as recited in claim 1. Furthermore, as indicated in page 7 of the Action, "Carman is silent on the encryption module comprises a symmetric encryption program." Therefore, Carman does not teach or suggest all limitations of claim 1.

In fact, Carman teaches away from "a host computing processor having a peripheral port, and operable to encrypt the list of passwords," as recited in claim 1. Particularly, Carman discloses that the "controller (105) performs the processes of the present invention that encrypt, decrypt, and verify the validity of any access requests to the memory (110)." (Paragraph [0022].) Therefore, Applicant contends that it would **not** have been obvious to one of ordinary skill in art to modify the teachings of Carman to include "a host computing processor having a peripheral port, and operable to encrypt the list of passwords," as recited in claim 1.

Claim 8 depends from claim 1, and is therefore patentable for the reasons set forth above.

Similarly, Carman makes no mention of among other things, "an encryption module executed on the computer and operable to encrypt a new password for addition to the list of passwords," as recited in claim 12. Claim 18 depends from claim 12, and is patentable for the reasons set forth above.

As noted above with claims 1 and 12, Carman makes no mention of, among other things, "encrypting a list of passwords at a host computing processor," as recited in claim 20. Claim 26 depends from claim 20, and is patentable for the reasons set forth above.

Claims 3, 11, 13, 19, 22, and 29

Claims 3, 11, 13, 19, 22, and 29 stand rejected under 35 U.S.C. § 103 (a) as being unpatentable over Carman in view of U.S. Patent No. 5,950,013 ("Yoshimura").

Yoshimura discloses a memory card having volatile memory that is used connected to a host system apparatus. Yoshimura makes no mention of, among other things, "a host computing processor having a peripheral port, and operable to encrypt the list of passwords," as recited in claim 1, "an encryption module executed on the computer and operable to encrypt a new password for addition to the list of passwords," as recited in claim 12, or "encrypting a list of passwords at a host computing processor," as recited in claim 20. Therefore, Yoshimura does not overcome the deficiencies of Carman with respect to the "operable to encrypt" limitation of claim 1, "encryption module" limitation of claim 12, and "encrypting" limitation of claim 20, respectively.

Claims 3 and 11 depend from claim 1, claims 13 and 19 depend from claim 12, and claims 22 and 29 depend from claim 20, and are therefore patentable for the reasons set forth above.

CONCLUSIONS

In light of the foregoing, Applicant respectfully submits that claims 1 – 29 are allowable. The undersigned is available for telephone consultation during normal business hours.

Respectfully submitted,

Daniel S. Jones
Reg. No. 42,697

File No. 066040-9765-00
Michael Best & Friedrich LLP
100 East Wisconsin Avenue
Suite 3300
Milwaukee, Wisconsin 53202-4108
414.271.6560
X:\CLIENTB\066040\9765\A2089371.2